MESSAGEPHONE, INC.

March 10, 1994

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
1919 M. Street, N.W.; Room 222
Washington, D.C. 20554

VIA FEDERAL EXPRESS

93-292

RE: Ex Parte Letter, CC Docket No. 92-77; Phase II

Dear Mr. Caton:

MessagePhone, Inc. ("MessagePhone"), a party to this proceeding, believes it would be remiss not to inform the Federal Communications Commission ("Commission") and the other parties that its two network architectures for offering Billed Party Preference ("BPP"), as described in Comments, Reply Comments, and ex parte letters,[1] also can be utilized to prevent many of the methods of telephone fraud described in the Commission's Common Carrier Docket 93-292.

Unlike other, more costly technical solutions for implementing BPP, both of MessagePhone's architectures are capable of providing numerous new basic and enhanced services not currently offered by local exchange carriers ("LECs"). If BPP is mandated by the Commission, LECs that implement one of

[1] See MessagePhone's Comments in the Matter of Billed-Party Preference for "0+" InterLATA Calls, July 6, 1992 ("Comments"); Reply Comments, August 27, 1992 ("Reply Comments"); Ex Parte letter from Douglas E. Neel to Ms. Donna Searcy, June 10, 1993 ("Ex Parte I"); Ex Parte letter from Douglas E. Neel to Mr. William Caton, August 6, 1993 ("Ex Parte II"). In this proceeding, MessagePhone has described both its Payphone Gateway Platform ("PGP") and its Billed Party Preference Platform ("BPP Platform"). The PGP resides on the line-side of the local exchange central office and consists of an intelligent line monitor, remote management system, and voice processing computer. See Comments at 18-22 for a detailed description of the PGP. The BPP platform resides as an adjunct to the local exchange carrier's equal access tandem switch and consists of a network interface, voice response unit, and central processor platform. See Ex Parte I at 5-8 and Ex Parte II at 4-6 for a description of the BPP platform.

MessagePhone's solutions will have the option of accessing many of the other revenue-generating services. Accordingly, the cost for the equipment will be allocated among the various services, thus reducing further the cost of implementing BPP, while generating new revenues for the local exchange carrier.

Even more important, the same architectures can be utilized to thwart many of the types of toll fraud described in docket 93-292. In particular, these architectures can be used to stop pay telephone "clip-on fraud," "shoulder surfing," and other types of Line Information Database ("LIDB") and calling card fraud.

A. Pay Telephone "Clip-on" Fraud

A growing percentage of pay telephones are "smart," i.e., pay terminals with internal intelligence and processing capability. These smart pay telephones can count coins, rate long distance calls, and process debit and calling card calls. Moreover, smart telephones are capable of automating even more complex operator functions, such as collect telephone calls. Because the billing is processed within the telephone, most calling card and collect calls enter the public network as 1+ calls. Understandably, the public telephone network does not know what kind of call is being processed and must "assume" that the caller has already paid for the call.

However, since the processing intelligence is located within the terminal, smart pay telephones are particularly susceptible to numerous problems, including increased fraud. One of the most common problems is "clip-on" fraud. With "clip-on" fraud, the caller clips a manual dialing device to the telephone line between the wall and the pay telephone. Then the caller can dial a 10XXX1+ long distance call and the telephone owner is responsible for the bill.

Because the telephone network is accessed in back of the telephone, the smart pay telephone cannot be utilized to detect the fraud. Likewise, the public network does not "know" what kind of call is being processed and cannot be utilized to detect the fraud. Both fraudulent and legal calls enter the public network from a smart pay telephone as 1+ calls. Accordingly, the network will be unable to determine whether the calls are illegal.

Pay telephone providers have two choices for identifying and stopping "clip-on" fraud. The smart pay telephone can be connected to the LEC's coin line and can utilize the operator services from an established operator service provider.[2] However, this option is unacceptable for most pay telephones. In many states, coin lines are available only for the LECs' pay telephones. Most smart pay telephones are not designed to utilize a coin line. In addition, many pay telephone providers do not want to utilize existing operator service providers, preferring to personally offer their own operator services.

MessagePhone's technology provides an alternative that does not require the use of a coin line or operator service provider and can detect and stop clip-on fraud. MessagePhone's PGP technology is capable of executing some of the processing functions for the smart pay telephone.[3] The line-side technology can monitor the telephone call, count and return coins, and differentiate between 0-, 0+, and 1+ calls. Moreover, the PGP can rate and process interLATA and automate operator calls. These basic services can be unbundled and purchased by pay telephone providers and used to offer a variety of enhanced and operator services. The PGP line-side technology will identify 10XXX1+ calls (including calls initiated from "clip-on" dialers) and require that the caller has pre-paid for the call (e.g., with coins or with a calling or debit card) before call completion. If the PGP does not detect payment (as with "clip-on" fraud), call progress is halted and the call is not completed.

The PGP also is capable of executing the same diagnostics used by coin lines to detect the "clip-on" dialer. Once detected, the PGP can initiate appropriate alarms. With either or both of these methods, the PGP can eliminate "clip-on" fraud.

If not stopped, it is likely that incidences of "clip-on" fraud will increase dramatically. Most of the Regional Bell Operating Companies ("RBOCs") recently have announced their intent to replace their existing base of pay telephones with

[2] The "coin line" is a specially treated telephone line that is capable of detecting and returning coins. Coin lines also have the diagnostic capability to detect "clip-on" dialers. The business lines used by smart pay telephones do not have this capability.

[3] MessagePhone's PGP technology gives the pay telephone provider a wide range of options. The PGP can assume all processing functions on a coin line or standard business line, or can execute only the processing functions desired by the pay telephone provider. This flexibility gives the provider the option to use smart telephones, semi-smart telephones, or standard "dumb" telephones; i.e., pay telephones with no processing capability.

expensive smart pay telephones.[4] All of these telephones will be susceptible to clip-on fraud. Clip-on fraud must be eliminated before the transition to smart pay telephones, or the rate base could become accountable for the expense of the fraud.

B. Shoulder Surfing

"Shoulder surfing" is one of the most financially devastating methods of telephone toll fraud. With "shoulder surfing," the criminal watches over a caller's shoulder while the caller inputs the calling card number and personal identification number ("PIN") with the pay telephone key pad. The perpetrator memorizes and uses the stolen calling card number fraudulently to pay for interLATA and international telephone calls.

Clearly, the most effective method to end "shoulder surfing" is to utilize pay telephones with card readers. Unfortunately, because of the high cost of card reader pay telephones, most pay telephone providers, including some LECs and long distance carriers ("IXCs"), have not replaced their existing base of standard pay telephones. Consequently, their customers remain vulnerable to toll fraud.

The primary reason that card reader pay telephones cost more than standard pay telephones is that the processor and intelligence for the card reader are located within the terminal. On average, the cost of the equipment is five to ten times higher than for standard pay telephone equipment. Because the processing intelligence is located outside the central office, the cost for maintenance also is considerably higher.

MessagePhone's PGP technology proffers two less expensive alternatives. First, instead of replacing all pay telephones with expensive equipment, LECs and other pay telephone providers can upgrade their existing base with an inexpensive retrofit card reader (in the upper housing of the telephone) and use the PGP line-side technology for calling and debit card processing. The retrofit/PGP combination could cost as much as $500 less PER TELEPHONE for the initial equipment investment than a smart card reader pay telephone. Because the PGPs are located in the controlled environment of a central office (or some other centralized location), maintenance expenses also will be greatly reduced.

[4] Smart pay telephones can cost five to eight times more than standard dumb pay telephones and require significantly more maintenance. However, the RBOCs might be relieved from their Open Network Architecture ("ONA") obligations if basic services are provided from the telephone rather than from the central office.

The second alternative also is available with the BPP Platform and is discussed in Section C below. The PGP line monitor is directly connected via a data link to a Remote Management System located in the originating LATA. Records of all transactions processed by the PGP, including all LIDB queries, are transmitted immediately to the Remote Management System. The Remote Management System has a special software algorithm that allows it to identify unusual account activity and warn the appropriate carrier.

C. Solutions for Other Methods of LIDB Fraud

MessagePhone's BPP Platform provides an alternative solution for fraud protection that works equally for pay and standard business and residential telephones. The LIDB does not have the capability of monitoring how often each account number is queried and utilized. Moreover, it would be burdensome and expensive to make additional modifications to the LIDB database. Because of these limitations, LIDB cannot be used to identify unusual increases in account activity and potentially stop fraudulent use.

The BPP Platform, with its line monitoring capability and main frame Call Processing Platform ("CPP"), has the ability to monitor and record LIDB queries. The BPP Platform's Intelligent Activity Profile application enables it to recognize a sudden increase in account activity and warn the appropriate service provider of the potential for fraud. The service provider can respond by calling the account holder and verifying that the calling card calls were approved. If the account holder verifies that the calls were unapproved and potentially fraudulent, either the LIDB or the CPP can be updated to show that the account is cancelled or temporarily suspended. A service similar to MessagePhone's Intelligent Activity Profile currently is used by major credit card companies (e.g., Visa and MasterCard) to decrease incidences of theft and fraud. MessagePhone's CPPs can be networked to provide either regional or national protection against fraud.

On occasion, the criminal has access to the credit or calling card number but must use a computer or guess in order to determine the correct PIN. A computer is used to attempt LIDB queries with all four digit combinations until the correct PIN is utilized. MessagePhone's BPP platform is able to track the number of incorrect PIN entries and, after a predetermined number of attempts (MessagePhone recommends three attempts), the BPP platform can withhold access to that account. As described above, the appropriate service provider is alerted and can contact the account holder in order to verify that the account is not being used illegally.

D. Conclusion

Telephone fraud is a serious problem that costs approximately $1 billion annually nationwide.[5] MessagePhone's technological solutions represent a major advancement toward abrogating the most common forms of toll fraud. Furthermore, by concomitantly implementing these services with BPP, the allocated cost of BPP to the LECs is reduced dramatically. As MessagePhone demonstrated, the properly allocated cost of BPP could be as low as $15 million per RBOC.[6]

Unfortunately, regulatory issues often are identified and solutions are implemented in a vacuum. Throughout this proceeding, MessagePhone has described more than two dozen basic and enhanced services made available with its technology that were not previously available. Most of these services also can be provided to other service providers (IXCs, pay telephone operators, etc.) through the Commission's ONA rules. Many of these providers want access to these new services. The Commission's mandate of BPP would enable the LECs to install equipment that would assure consumers equal access to their operator service provider of choice, greatly reduce incidences of toll fraud, and provide numerous new revenue-generating services.

Sincerely,

Douglas E. Neel

Douglas E. Neel
V.P., Regulatory Affairs

Enclosed: Two Additional Copies

cc: Reed E. Hundt
Andrew C. Barrett
James H. Quello
Gary Phillips
Mark Nadel

[5] "New York Telephone Cracks Down On Phone Fraud," *Phone+*, Aug. 1992, at 18.

[6] *See* Comments at 23-28; Reply Comments at 18-26; Ex Parte I at 2-4, 6-8.